Contactless data carrier

[001]The present invention relates to an apparatus as well as a method for reliably determining the deliberate use of a contactless data carrier.

[002]The term "contactless data carrier" or "contactless card" used in the following refers to all arrangements, which have a microchip and an antenna connected to it and are adapted to exchange data with a suitable reading device. These include, beside chip cards for payment applications, contactlessly readable identification documents, such as passports and identity cards with built-in microchip as well as, furthermore, RFID labels.

[003]Contactless data carriers for payment transactions today are exclusively used in closed applications, such as for instance for paying in the canteen or in public transport. The reason for this is that in Germany contactless cards are still not permitted for payment applications, as e.g. in the form of a cash card, which is due to security reasons. The decisive factor for this is the fear that third persons may contactlessly discharge a cash card unnoticed by the card holder. For example, it is thinkable, that with the help of a mobile terminal for contactless cards, which is moved through crowds of people (e.g. fairs, concerts, underground, train station ...), "electronic" money is unnoticedly debited from the wallets located in the vicinity. With contact-type cards such a problem does not occur, since a payment transaction is effected by the card holder by inserting the card into the card reader.

[004]Beside the use as a means of payment contactless cards likewise can be employed as data carriers in documents of value, such as e.g. passports. In particular, it is expedient to use contactless cards as visa, which can be incorporated, for example bonded, into the passport document. For this purpose e.g. the coil-on-chip method (CoC) is suitable, with which the antenna is disposed on the chip. But conventional contactless arrangements can be used likewise, such as e.g. foils with chip disposed thereon and a coil printed onto the foil.

[005]When using contactless cards in documents of value, the problem arises, that an unintended reading by third parties is to be prevented. The same applies to the unauthorized and unnoticed readout of contactless transponders, which are employed for product identification.

[006]Therefore, it is the problem of the present invention to provide an apparatus as well as a method for reliably determining the deliberate use of a contactless data carrier by the card holder.

[007]The problem is solved by the features of the independent claims. In claims dependent on these are specified advantageous embodiments and developments of the invention.

[008]With the help of the additional data transmission channel by optical means data are exchanged between reading device and data carrier, which are suitable to perform an authentication between reading device and contactless card. The authentication via the additional data transmission channel prevents an unintentional actuation of the contactless card, since the optical information is not available, when the data carrier is not optically visible to the reading device, for instance is carried in a bag/purse.

[009]According to a first embodiment of the invention the data carrier has optically readable information, such as e.g. a bar code or matrix code. When the card is presented to the reading device, this information is read and evaluated by means of an optical reading device, e.g. a bar code scanner. The optically read information then can be used by the contactless data carrier for authenticating purposes between itself and the contactless reading device, in order to in such a way furnish the authorization for a subsequent transaction.

[0010]An enhancement of this first embodiment is to output the optically shown information onto a display device, e.g. a LCD display, by means of the chip. As a result of this, simply copying the information is no longer possible, since the information may contain randomly generated data structures.

[0011]According to a further embodiment of the invention the contactless data carrier is equipped with an optical illuminant, e.g. an IR light emitting diode or a light emitting foil. The illuminant can have an electrical connection to the chip or can be integral part of the chip. As soon as a contactless reading device intends to perform a transaction with the data carrier, the illuminant is used for sending additional data from the chip to the reading device by optical means. These data can be part of a mutual authentication and are used according to the invention for releasing a subsequent transaction. When the reading device does not have knowledge of the optically transmitted data, a transaction with the data carrier cannot be carried out.

[0012]Preferably, changes of the environmental conditions can be detected on the data carrier, as soon as the data carrier is removed from the bag for a payment transaction. For example, by means of a light-sensitive optical component (14) can be determined, whether the card is located inside a bag or outside. The light-sensitive component can have an electrical connection to the chip or be integral part of the chip. As soon as the light-sensitive component is exposed to a minimum of brightness, according to the invention a release signal is produced, which permits a transaction between the chip and the contactless reading device.

[0013]The advantage of this variant is that special contactless terminals are not required, and the already existing infrastructure (e. g. contactless terminals, as they are already used in closed systems, such as a canteen) can still be used.

[0014]A development of this idea provides that the reading device itself produces an optical signal. For releasing a transaction by means of the chip it is thinkable to provide the optical signal with a striking modulation, e.g. a 1-kilohertz-signal, or to transmit data to the chip by means of the optical signal, this data being used for an authentication between data carrier and reading device.

[0015]A combination of the above-mentioned embodiments consists of providing both an optical illuminant and an optical receiving means on the card and to connect them to the chip or to provide these means as integral parts of the chip. In this

case beside a contactless bi-directional data transmission additionally a bi-directional optical data transmission between the card and a reading device would be practicable. According to the invention it is provided to switch between the different transmission channels, preferably each transmission channel can be used at least one time for the transmission of data.

[0016]A further advantage of this arrangement is that the energy for operating the optical means of communication is obtained from the contactless transmission channel (e. g. magnetic or capacitive coupling). Furthermore, it is understood, that for the optical communication beside visible light also IR, UV or a mixture (uplink vs. downlink) from these areas can be used.

[0017]Analogously to optical information, alternatively or additionally, acoustic information may be used, e.g. in the form of transmitting an encoded acoustic signal, which e.g. can be produced by means of a loudspeaker integrated in the card (e.g. piezo loudspeaker).

[0018]Furthermore, a loudspeaker located in the card is suitable for acknowledging each payment transaction with a signal, which indicates to the card holder that in this moment a payment transaction takes place on his card. In this embodiment of the invention though it would still be possible to illegally debit money from the card with a mobile contactless terminal, such a transaction would not remain unnoticed.

[0019]Instead of a loudspeaker, alternatively or additionally, there can be provided to equip the data carrier with a vibration alarm.

[0020]In the following the invention is explained in detail with reference to the embodiments represented in the figure.

[0021]Fig. 1 shows an embodiment of the present invention, wherein onto the data carrier is applied an optical information,

[0022]Fig. 2 shows a further embodiment of the invention with an illuminant disposed on the data carrier,

[0023]Fig. 3 shows a further embodiment of the invention with an optical receiving means disposed on the data carrier,

[0024]Fig. 4 shows a further embodiment of the invention with an optical component disposed on the data carrier,

[0025]Fig. 5 shows an embodiment of a method for deriving a cryptographic key, and

[0026]Fig. 6 shows an embodiment of an authentication method.

[0027]Fig. 1 shows a contactless data carrier 1a, with an antenna 2 disposed thereon and a chip 3 electro-conductively connected with it. An area of the data carrier has optical information 4, for example a bar code or a matrix code, which is suitable for being transmitted to the reading device 1 via an optical data transmission channel 5. The optical data transmission channel 5 is provided additionally to the antenna-based contactless data transmission channel 15.

[0028]Fig. 2 describes a contactless data carrier, on which an optical illuminant 6 is disposed. The illuminant 6, which can be designed as a LED, OLED or also as an infrared light emitting diode (IR-LED), is electro-conductively connected, as indicated by the arrow 7, to the chip 3 and is activated by it. Here an optical data transmission is effected via the data transmission channel 8.

[0029]A further embodiment is shown in Fig. 3, wherein on the data carrier 1a is disposed an optical receiving means 9, which is electro-conductively connected to the chip 3 and enables a bi-directional optical data transmission between reading device 1 and data carrier 1a. The chip 3 is adapted to control the data transmission for both the contactless data transmission 15 and the optical data transmission 10. The two transmission channels can be operated alternately or

simultaneously. Furthermore, the transmission channels can be operated in a flat or hierarchical (master-slave) fashion.

[0030]With the help of the optical component 14 represented in Fig. 4, which has an electro-conductive connection 11 to the chip 3, with sufficient incidence of light 13 the data transmission via the antenna-based contactless interface can be released (indicated by the arrow 12).

[0031]The method for releasing secret information stored in the data carrier 1a can be executed for example as follows. As represented in Fig. 5, the storage device 21 of the chip 3 has a plurality of storage areas 24 or 22, which partially are freely readable and the contents of which partially are protected against an unauthorized readout by means of suitable keys. The protected storage area 22 contains at least one data record 23, which consists of information to be kept secret, such as e.g. biometric data, PIN etc. The freely readable storage area 24 contains at least one data record 25, which is unequivocally allocated to the respective data record 23 and represents a compression value, e.g. a CRC, hash, a cryptographic check sum etc. A conclusion drawn from the content of the freely readable data record 25 about the content of the secret data record 23 is impossible.

[0032]For reading out one of the data records 23 according to the invention it is provided, that in a first procedure step the data record 25 allocated to the data record 23 is read out via the antenna-based data transmission channel 15 and the optically readable information 20 of the data carrier 1a, e.g. a bar code or a MRZ (machine readable zone) is read out with the aid of the reading device 1.

[0033]In a second procedure step from the data record 25 and the optically readable information 20 a cryptographic key 26 is derived. For this purpose any key derivation methods can be employed, which are sufficiently well-known from the prior art, such as e.g. key derivation using a master key etc. The cryptographic key individual for the data carrier, which has been derived from the secret master key, is already stored on the data carrier. The master key is

deposited in the reading device for deriving the cryptographic key 26 by means of the optically read information 20 and the contactlessly read data record 25.

[0034]A third procedure step provides to perform an authentication 27 between reading device 1 and the chip 3 of the data carrier 1a by means of the derived cryptographic key. By this means it is verified, whether the respective keys known to the reading device 1 or stored in the data carrier 1a are identical. An authentication method already known from prior art works according to the "challenge-response principle", which is widely used in the field of chip cards. By a "get-challenge" command the reading device 1 receives a random number from the chip 3, so as to then authenticate itself to the chip by the data of an "external authenticate" command, which are derived from the random number and the key. It is obvious that further authentication steps, for example for the mutual authentication, and other methods for authentication can be used.

[0035]In a simplified method in the third procedure step the reading device which uses the two data transmission channels shall merely authenticate itself as such, without simultaneously proving the knowledge of a secret key. In the second procedure step 26 for example then a value is derived, which though it is used as a key for the third step 27, it is not secret or derived from a master key.

[0036]In an optionally last procedure step from the read-out data record 23 a compression value is formed and this compression value is compared to the content of the freely readable data record 25 (cf. Fig. 5, verify 28). If the two compression values differ from each other, then it is to be assumed, that the data record 23 has been unauthorizedly changed. After a successful authentication the data record 23 can be read out.

[0037]The method described in Fig. 6 likewise provides that at least for a part of the data stored in the transponder the access is permitted only upon successful authentication. This method, too, works according to the "challenge-response principle".

[0038]In a first step 30 the reading device 1 requests a random number from the data carrier 1a via the antenna-based transmission channel 15. In an embodiment according to the invention a random number generated by the data carrier 1a is transmitted via the optical data transmission channel 5, for example a (infrared-/UV-) LED, to the reading device 1 (step 31: "response"). A further possibility is to output the random number in the form of a bar code, pixel code, MRZ (machine readable zone) onto a display 4 on the contactless data carrier 1a. Simultaneously a response can be sent via the antenna-based data transmission channel 15, which differs in content from the contactless data transmitted by optical means, but avoids a time-out in the transmission channel, i.e. in particular at the reading device. On the one hand a potential attacker cannot draw any conclusions as to content when eavesdropping on the antenna-based transmission channel 15, and on the other hand a special treatment of individual application commands is not required, so that the software of the reading device 1 has not to be modified. For example, it is expedient to send the code "90 00" (command successfully carried out). In order to mislead possible attackers also wrong data can be transmitted.

[0039]Likewise, it is possible to request the random number via the optical data transmission channel and to transmit it via the antenna-based data transmission channel.

[0040]Then the authentication algorithm is executed according to the known method for the one-sided or mutual authentication ("external authenthicate", 32). After the successful completion of the authentication process, the actual communication 33 can be started and the data record 23 is read out.

[0041]The method described with respect to Fig. 6 can be used in combination with or independently of the method described in Fig. 5.

[0042]An advantage of the described method is that by using two different data transmission channels - namely the optical 5 and the antenna-based 15 - a tampering with or replacement of the data is made significantly more difficult. Therefore, it is especially suitable for the exchange of sensible data, such as e.g.

personal data. A one-sided authentication or a mutual authentication are improved by the combined use of the two data transmission channels.

[0043]Depending on the type of data to be transmitted it is also possible to selectively use only one data transmission channel. The loss of security connected therewith normally is coupled with an increase of processing speed and may be tolerated with data as needed for example for the fields of logistics, transport of goods and merchandise management. If with the same data carrier 1a also sensible data are to be processed, there can be mandatory provided to use the two data transmission channels when reading out by means of the reading device. The switching between one- or two-transmission-channel modus can be effected automatically after having set a flag or the like.

[0044]A reading device 1 according to the invention is an intelligent device, which is equipped with both antenna-based contactless reading means 2 and optical reading means. In a preferred embodiment the reading device 1 is formed as a mobile terminal, e.g. mobile phone, PDA, laptop or the like and has an interface for contactless communication, such as NFC (near field communication). As an optical means of communication the IRDA interface present in most of the devices can be used. As an optical reading means a camera can be provided. Preferably, the optically readable data, such as e.g. the serial number of the chip 3 on the data carrier 1a are represented in a machine readable form (bar code, OCR data). Such a reading device 1 is especially suitable for checking travel documents by police or border police, and via a possibly additionally existing online connection further information can be requested.

[0045]For increasing the security there can be provided, that the chip 3 of the data carrier 1a additionally generates a random number serving as a serial number and that it transmits this number via the antenna-based data transmission channel to the reading device 1. The use of such random serial numbers is described, for example, in ISO 14443 (Chapter 6.6.4, "UID contents and cascade levels"). The serial number of the data carrier 1a required for carrying

out the anticollision algorithm here is not formed by an unequivocal and unmistakable number, as it is usual, but by a random number freshly produced for each transaction. By this measure a conclusion drawn from the serial number about the identity of the data carrier is not possible. A possible (replay-) attack by repeating a once eavesdropped communication between data carrier and terminal can be prevented especially effective by this means.

[0046]Likewise, the optically readable data can be available on the data carrier 1a in a non-static fashion and be dynamically modified e.g. with the aid of a display or the like. In such a way also single-use passwords, random serial numbers etc. can be generated and displayed. Furthermore, any combination of the dynamically generated data and either antenna-based or optically transmitted data is thinkable.

[0047]According to the present invention a contactless data carrier has an antenna and a chip, the data carrier having means for the transmission of data via an optical data transmission channel and means for the transmission of data via an antenna-based data transmission channel. On the data carrier are disposed data, which via the optical data transmission channel and/or the antenna-based data transmission channel are transmittable to a reading device.